Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

28 November 2018

PIN Number
20181128-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

The following information is being provided by the FBI, with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided in order to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber criminals.

This PIN has been released **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

UPDATE: Initial Intrusion Activities of SamSam Ransomware Actors Magnify Exploitation of Victim Network Vulnerabilities

This report is an update to the FLASH released on 25 March 2016, Alert Number MC-000070-MW.

Summary

This update is to provide information about the vulnerabilities and exploits used to deploy SamSam ransomware, also known as MSIL/Samas.A, by cyber criminals Mohammad Mehdi Shah Mansouri and Faramarz Shahi Savandi. On 26 November 2018, the District of New Jersey indicted Mansouri and Savandi for developing and deploying SamSam ransomware. SamSam infects whole networks and encrypts victim data, allowing Mansouri and Savandi to demand considerable ransoms in Bitcoin in return for decryption keys.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat

The SamSam actors targeted a wide variety of sectors, including critical infrastructure, predominately in the United States, but also in Europe and other parts of the world. In providing essential functions, such organizations have a critical need to resume operations quickly and are more likely to pay large ransoms. Network-wide infections against organizations are far more likely to garner large ransom payments than campaigns targeted at individuals.

Technical Analysis

The actors exploit Windows servers to gain persistent access to a victim network and infect all reachable hosts. In early 2016, victims reported the JexBoss Exploit Kit was used to access vulnerable JBOSS applications. Since mid-2016, analysis of victim machines indicates the perpetrators use the Remote Desktop Protocol (RDP) to gain persistent victim network access via brute force attacks or using stolen/purchased login credentials. Using RDP for intrusion presents a challenge because the malware enters through an approved access point, thereby decreasing the likelihood of detection.

After gaining network access, the SamSam actors escalate privileges for administrator rights, drop malware onto the server, and run an executable file, all without victim action or authorization. While many ransomware campaigns rely on a victim completing an action, such as opening an email or visiting a compromised website, RDP allows cyber actors to infect victims with minimal detection.

Analysis of tools found on victim networks indicated the actors purchased several of the stolen RDP credentials from known darknet marketplaces. Analysis of victim access logs revealed the SamSam actors can infect a network within hours of purchasing the credentials. During remediation, several victims found suspicious activity on their networks unrelated to SamSam, a possible indicator the victim's credentials were stolen, sold on the darknet, and used for other illegal activity.

SamSam actors leave ransom notes on encrypted computers, which instruct victims to establish contact through a Tor hidden service site. After paying the ransom in Bitcoin and establishing contact, victims receive links to download cryptographic keys and tools to decrypt their network.

Recommended Mitigations

The following list includes self-protection strategies against MSIL/Samas.A ransomware campaigns:

- Audit your network for systems using RDP for remote communication. Disable the service if unneeded or install available patches. Users may need to work with their technology vendors to confirm that patches will not affect system processes.
- Verify all cloud-based virtual machine instances with a public IP do not have open RDP ports, specifically port 3389, unless there is a valid business reason to do so. Place any system with an open RDP port behind a firewall and require users to use a Virtual Private Network (VPN) to access it through the firewall.
- Enable strong passwords and account lockout policies to defend against brute-force attacks.
- Apply two-factor authentication, where possible.
- Apply system and software updates regularly.
- Maintain a good back-up strategy.
- Enable logging and ensure logging mechanisms capture RDP logins. Keep logs for a minimum of 90 days and review them regularly to detect intrusion attempts.
- When creating cloud-based virtual machines, adhere to the cloud provider's best practices for remote access.
- Ensure third parties that require RDP access are required to follow internal policies on remote access.
- Minimize network exposure for all control system devices. Where possible, critical devices should not have RDP enabled.

- Regulate and limit external to internal RDP connections. When external access to internal resources is required, use secure methods such as VPNs, recognizing VPNs are only as secure as the connected devices.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

For comments or questions related to the content or dissemination of this product, contact CyWatch.

Your Feedback Regarding this Product is Critical

Please take a few minutes to send us your feedback. Your feedback submission may be anonymous. We read each submission carefully, and your feedback will be extremely valuable to the FBI. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to these products. Feedback may be submitted online here: https://www.ic3.gov/PIFSurvey